

REMARKS / ARGUMENTS

In the Office Action dated December 8, 2010, the Examiner rejected claims 1 - 5, 9 - 17, 21 - 25, and 30 and objected to claims 1, 10, 13, and 30. In response to the Office Action, the Examiner's claim rejections have been considered. Applicant respectfully traverses all rejections regarding all pending claims and earnestly solicits allowance of these claims.

1. Claim Objections

In sections 8 of the Office Action the Examiner objected to claims 1, 10, 13, and 30 for informalities. Applicant is amending the claims 1, 10 and 13 accordingly and canceling claim 30 and therefore requests withdrawal of the objections.

2. Claim Rejections - 35 U.S.C. §101

In section 10 of the Office Action, the Examiner rejected claim 30. Applicant is canceling claim 30, therefore rendering the rejection moot.

3. Claim Rejections - 35 U.S.C. §103

In sections 11 - 14 of the Office Action, the Examiner rejected all pending claims under 35 U.S.C. §103 (a). Specifically, the Examiner rejected claim 1 as being unpatentable over Bush in view of Shefi.

Applicant submits that claim 1 is patentable over the cited references whether considered independently or in combination by at least reciting:

A method for encrypting a digital data stream comprising the following steps:
 providing a communication device which has an interface for a digital storage medium, whose content may be read out and duplicated;
 providing the digital storage medium which is connected to the interface;
 storing a supply of symbols for encryption on the digital storage medium;
 providing a first random generator on the communication device which determines addresses on the digital storage medium;
 reading out the symbols from the digital storage medium using the addresses on the digital storage medium; and
 employing the read out symbols for encrypting or decrypting the digital data stream of the communication device.

As acknowledged by the Examiner, Bush fails to disclose at least “providing a first random generator on the communication device which determines addresses on the digital storage medium”. According to the Examiner this feature is taught by Shefi. With all due respect, Applicant disagrees.

Shefi addresses the technical problem of one-time pads, i.e. that “both parties must have the same physical pad of paper or diskette before communication can occur, thereby restricting communication to parties which have made the necessary arrangements in advance” (col. 3, lines 50-54). In other words, Shefi tries to remove the need for physical “one-time pads”. Shefi suggests the use of an electronic “one time pad” to solve the above technical problem (col. 3, lines 65-67). In particular, Shefi suggests generating true random numbers at a first and a second location, and ensuring that the true random numbers are identical at both locations. These identical true random numbers are used to generate identical electronic one-time pads at the first and at the second location (col. 4, lines 7-64). In other words, Shefi teaches the generation of random numbers in order to build “one-time pads”. As a result, Shefi removes the need for physical “one-time pads”.

Shefi does not, however, teach the step of “providing a first random generator on the communication device which determines addresses on the digital storage medium”. In other words, Shefi does not teach the use of a first random generator to select a particular symbol from the supply of symbols, and to thereby enable the multiple use of one-time pads (see page 3, lines 25-30 of the present patent application). As a matter of fact, Shefi addresses a fundamentally different technical problem than the present patent application. That is, Shefi addresses the technical problem of removing the need for “physical one-time pads” altogether, wherein the claimed invention addresses the technical problem of using “physical one-time pads” more efficiently. Consequently, a person skilled in the art does not receive any hints from Bush or Shefi to the technical problem of the claimed subject-matter. Neither Bush nor Shefi provide the person of ordinary skill in the art with any hints towards the claimed solution to the technical problem.

As outlined above, Shefi addresses the technical problem of providing “one-time pads” to a plurality of locations and suggests the uses of randomly generated “electronic one-time pads”. As a result, the method of Shefi removes the needs to distribute “one-time pads” to the plurality of locations. Consequently, a person of ordinary skill in the art applying the teaching of Shefi to

Bush would replace the physical “one-time pads” 102 of Bush with the electronic “one-time pads” taught by Shefi.

The person of ordinary skill in the art would not, however, arrive at the claimed subject-matter. In particular, the person of ordinary skill in the art would not arrive at the step of “providing a first random generator on the communication device which determines addresses on the digital storage medium”. As indicated above, the step of “providing a first random generator on the communication device which determines addresses on the digital storage medium” ensures that a particular “supply of symbols” or “one-time pad” can be used multiple times for encryption. That is, the distinguishing method step ensures that the “supply of symbols” may be used more efficiently. This technical problem is neither addressed nor solved by any one of Bush or Shefi.

As such, it must be noted that even a combination of the teachings of Bush and Shefi would not have provided the person of ordinary skill in the art with sufficient teaching to arrive at the claimed subject-matter. Consequently, the subject-matter of claim 1 is not obvious. Accordingly, Applicant requests withdrawal of the rejection of claim 1.

As claim 13 recites limitations similar to claim 1, Applicant request withdrawal of the rejection of claim 13 for the same reasons cited above.

The remaining claims are patentable by virtue of their dependency and for reciting additional limitations.

CONCLUSION

Applicant has made an earnest and *bona fide* effort to clarify the issues before the Examiner and to place this case in condition for allowance. Reconsideration and allowance of all of claims is believed to be in order, and a timely Notice of Allowance to this effect is respectfully requested.

The Commissioner is hereby authorized to charge any additional required fees from Deposit Account No. 50-2586, Deposit Account Name PERKINS COIE LLP.

Should the Examiner have any questions concerning the foregoing, the Examiner is invited to telephone the undersigned attorney at +1.206.359.3535.

Respectfully submitted,

Appl. No. 10/598,832
Amdt. Dated June 8, 2011
Reply to Office Action of December 8, 2010

Docket No. 73408.8001.US00

Date: June 8, 2011

/Aaron Wininger, Reg. No. 45,229/
Aaron Wininger
Reg. No. 45,229
PERKINS COIE LLP
1201 Third Avenue
Suite 4800
Seattle, WA 98101-3099